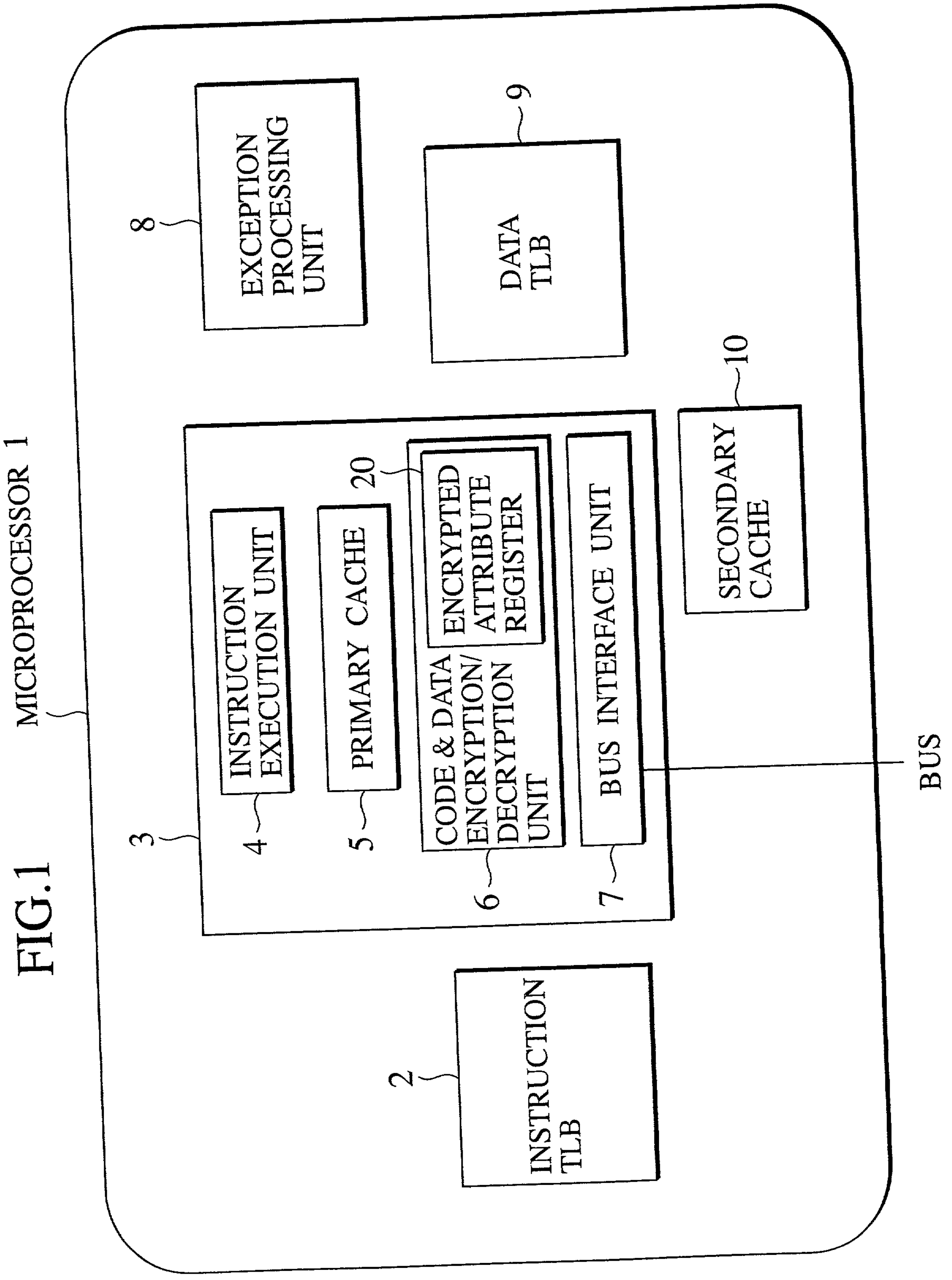
OBLON, SPIVAK, ET AL
DOCKET #: 217811US2RD
INV: Keiichi TERAMOTO, et al.
SHEET 1 OF 8

FIG.1


MICROPROCESSOR 1
2
INSTRUCTION TLB
3
4
INSTRUCTION EXECUTION UNIT
5
PRIMARY CACHE
6
CODE & DATA ENCRYPTION/ DECRYPTION UNIT
20
ENCRYPTED ATTRIBUTE REGISTER
7
BUS INTERFACE UNIT
8
EXCEPTION PROCESSING UNIT
9
DATA TLB
10
SECONDARY CACHE
BUS

10028794.122801

FIG.2

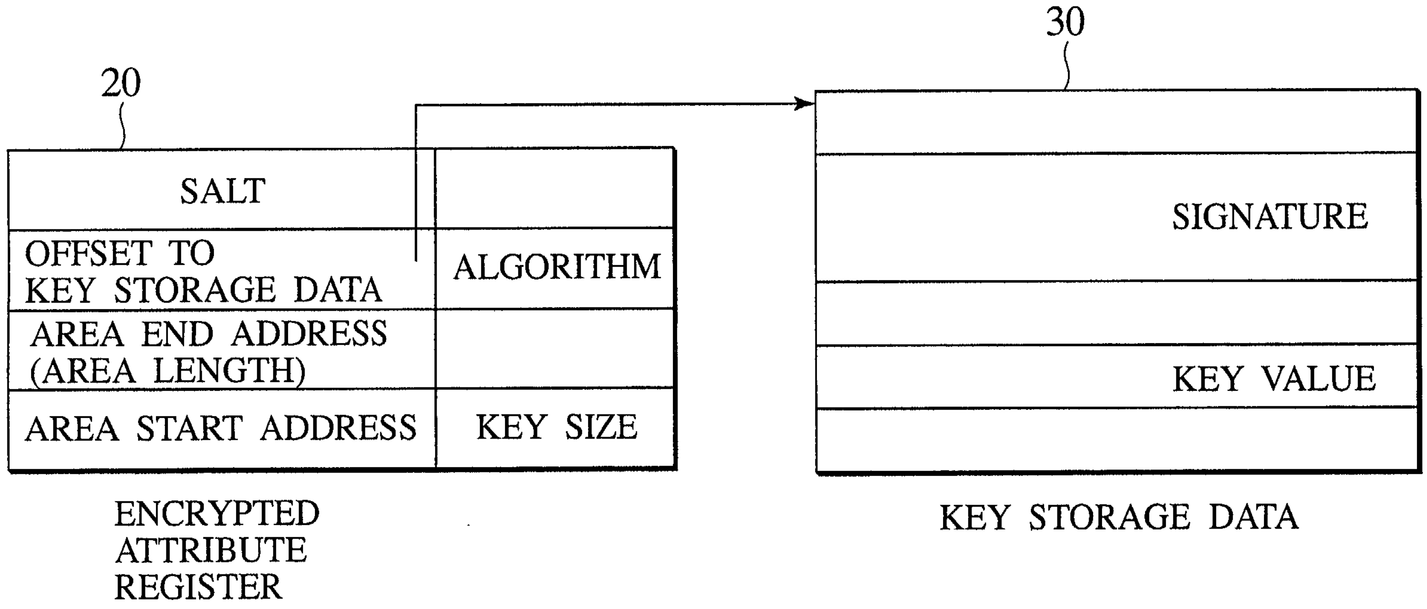
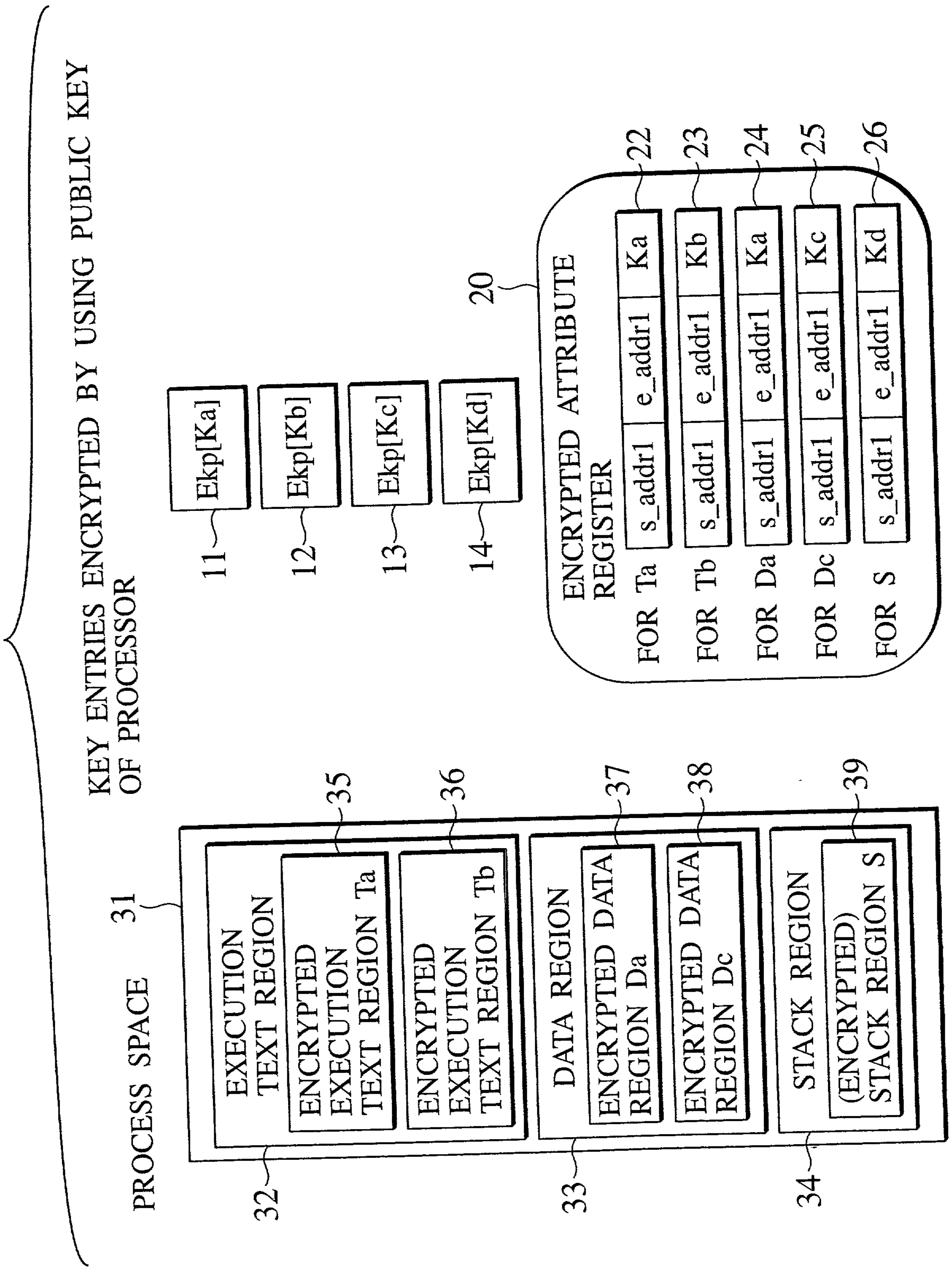
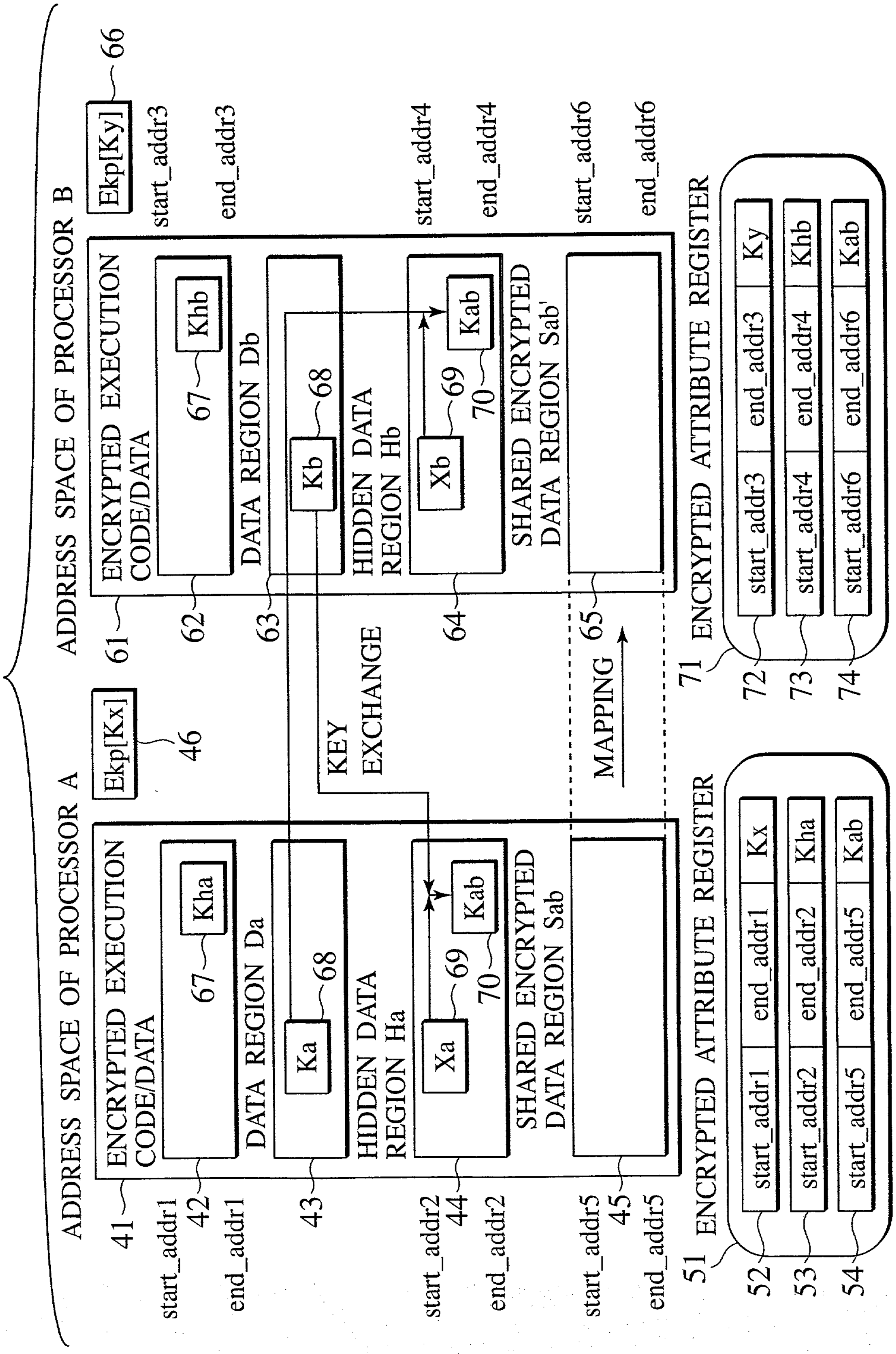

20
SALT
OFFSET TO KEY STORAGE DATA
ALGORITHM
AREA END ADDRESS (AREA LENGTH)
AREA START ADDRESS
KEY SIZE
ENCRYPTED ATTRIBUTE REGISTER
30
SIGNATURE
KEY VALUE
KEY STORAGE DATA

FIG.3


KEY ENTRIES ENCRYPTED BY USING PUBLIC KEY OF PROCESSOR
Ekp[Ka]
Ekp[Kb]
Ekp[Kc]
Ekp[Kd]
11
12
13
14
20
ENCRYPTED ATTRIBUTE REGISTER
FOR Ta
FOR Tb
FOR Da
FOR Dc
FOR S
s_addr1
e_addr1
Ka
Kb
Ka
Kc
Kd
22
23
24
25
26
PROCESS SPACE
31
EXECUTION TEXT REGION
ENCRYPTED EXECUTION TEXT REGION Ta
ENCRYPTED EXECUTION TEXT REGION Tb
35
36
32
DATA REGION
ENCRYPTED DATA REGION Da
ENCRYPTED DATA REGION Dc
37
38
33
STACK REGION
(ENCRYPTED) STACK REGION S
39
34

10022794.102802

FIG.4



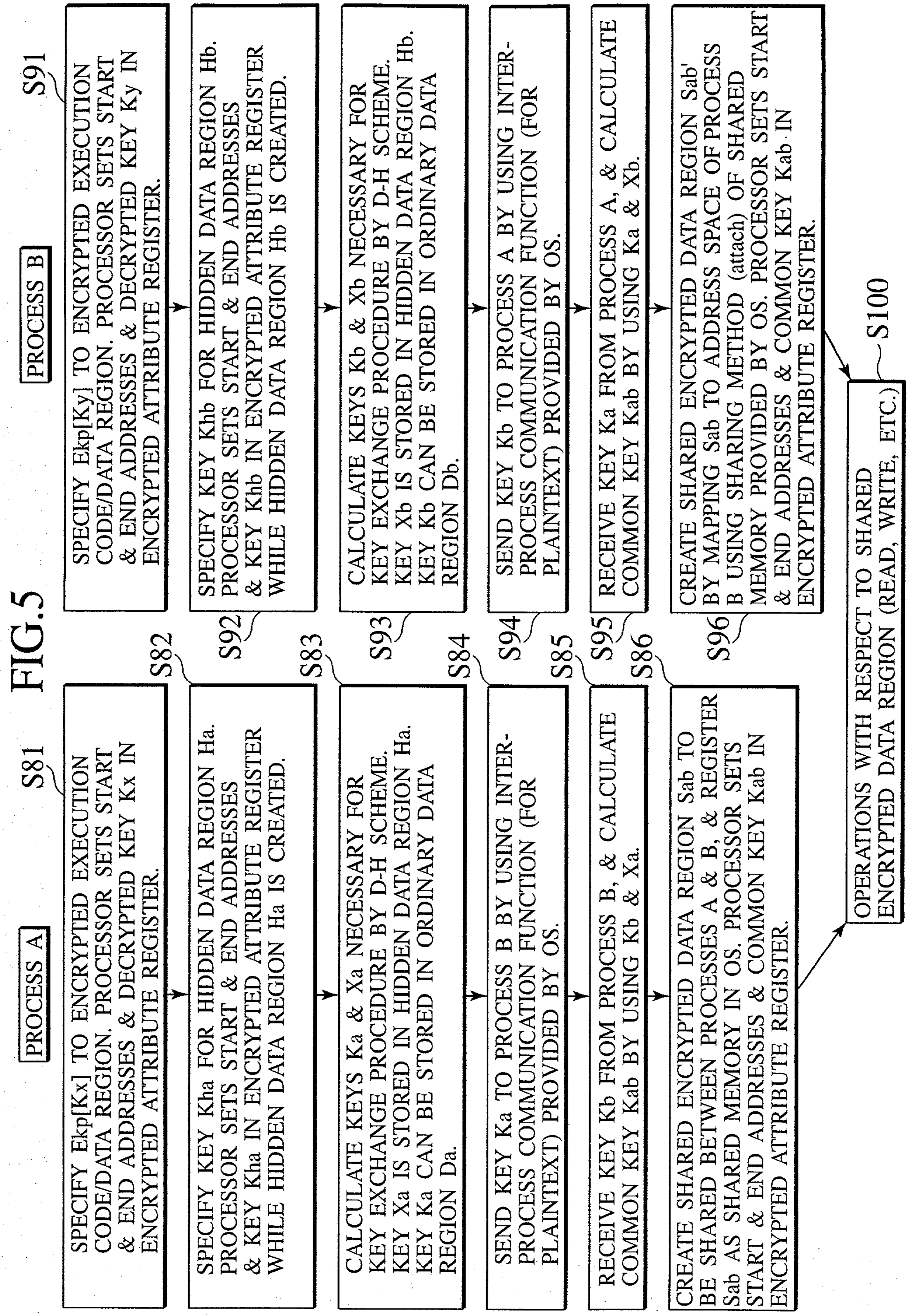
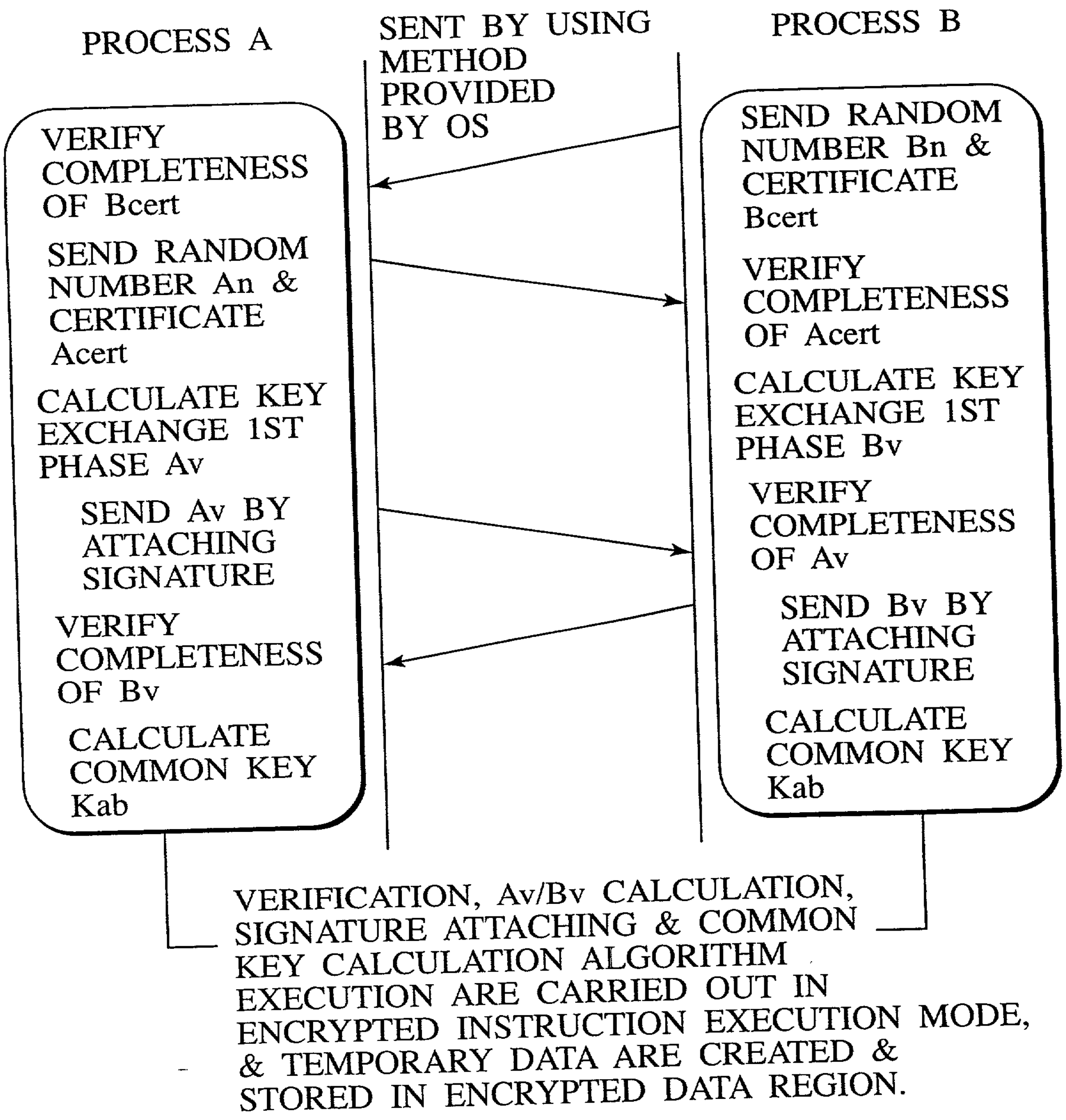


FIG.5

PROCESS A
S81
SPECIFY Ekp[Kx] TO ENCRYPTED EXECUTION CODE/DATA REGION. PROCESSOR SETS START & END ADDRESSES & DECRYPTED KEY Kx IN ENCRYPTED ATTRIBUTE REGISTER.
S82
SPECIFY KEY Kha FOR HIDDEN DATA REGION Ha. PROCESSOR SETS START & END ADDRESSES & KEY Kha IN ENCRYPTED ATTRIBUTE REGISTER WHILE HIDDEN DATA REGION Ha IS CREATED.
S83
CALCULATE KEYS Ka & Xa NECESSARY FOR KEY EXCHANGE PROCEDURE BY D-H SCHEME. KEY Xa IS STORED IN HIDDEN DATA REGION Ha. KEY Ka CAN BE STORED IN ORDINARY DATA REGION Da.
S84
SEND KEY Ka TO PROCESS B BY USING INTER-PROCESS COMMUNICATION FUNCTION (FOR PLAINTEXT) PROVIDED BY OS.
S85
RECEIVE KEY Kb FROM PROCESS B, & CALCULATE COMMON KEY Kab BY USING Kb & Xa.
S86
CREATE SHARED ENCRYPTED DATA REGION Sab TO BE SHARED BETWEEN PROCESSES A & B, & REGISTER Sab AS SHARED MEMORY IN OS. PROCESSOR SETS START & END ADDRESSES & COMMON KEY Kab IN ENCRYPTED ATTRIBUTE REGISTER.
PROCESS B
S91
SPECIFY Ekp[Ky] TO ENCRYPTED EXECUTION CODE/DATA REGION. PROCESSOR SETS START & END ADDRESSES & DECRYPTED KEY Ky IN ENCRYPTED ATTRIBUTE REGISTER.
S92
SPECIFY KEY Khb FOR HIDDEN DATA REGION Hb. PROCESSOR SETS START & END ADDRESSES & KEY Khb IN ENCRYPTED ATTRIBUTE REGISTER WHILE HIDDEN DATA REGION Hb IS CREATED.
S93
CALCULATE KEYS Kb & Xb NECESSARY FOR KEY EXCHANGE PROCEDURE BY D-H SCHEME. KEY Xb IS STORED IN HIDDEN DATA REGION Hb. KEY Kb CAN BE STORED IN ORDINARY DATA REGION Db.
S94
SEND KEY Kb TO PROCESS A BY USING INTER-PROCESS COMMUNICATION FUNCTION (FOR PLAINTEXT) PROVIDED BY OS.
S95
RECEIVE KEY Ka FROM PROCESS A, & CALCULATE COMMON KEY Kab BY USING Ka & Xb.
S96
CREATE SHARED ENCRYPTED DATA REGION Sab' BY MAPPING Sab TO ADDRESS SPACE OF PROCESS B USING SHARING METHOD (attach) OF SHARED MEMORY PROVIDED BY OS. PROCESSOR SETS START & END ADDRESSES & COMMON KEY Kab IN ENCRYPTED ATTRIBUTE REGISTER.
S100
OPERATIONS WITH RESPECT TO SHARED ENCRYPTED DATA REGION (READ, WRITE, ETC.)

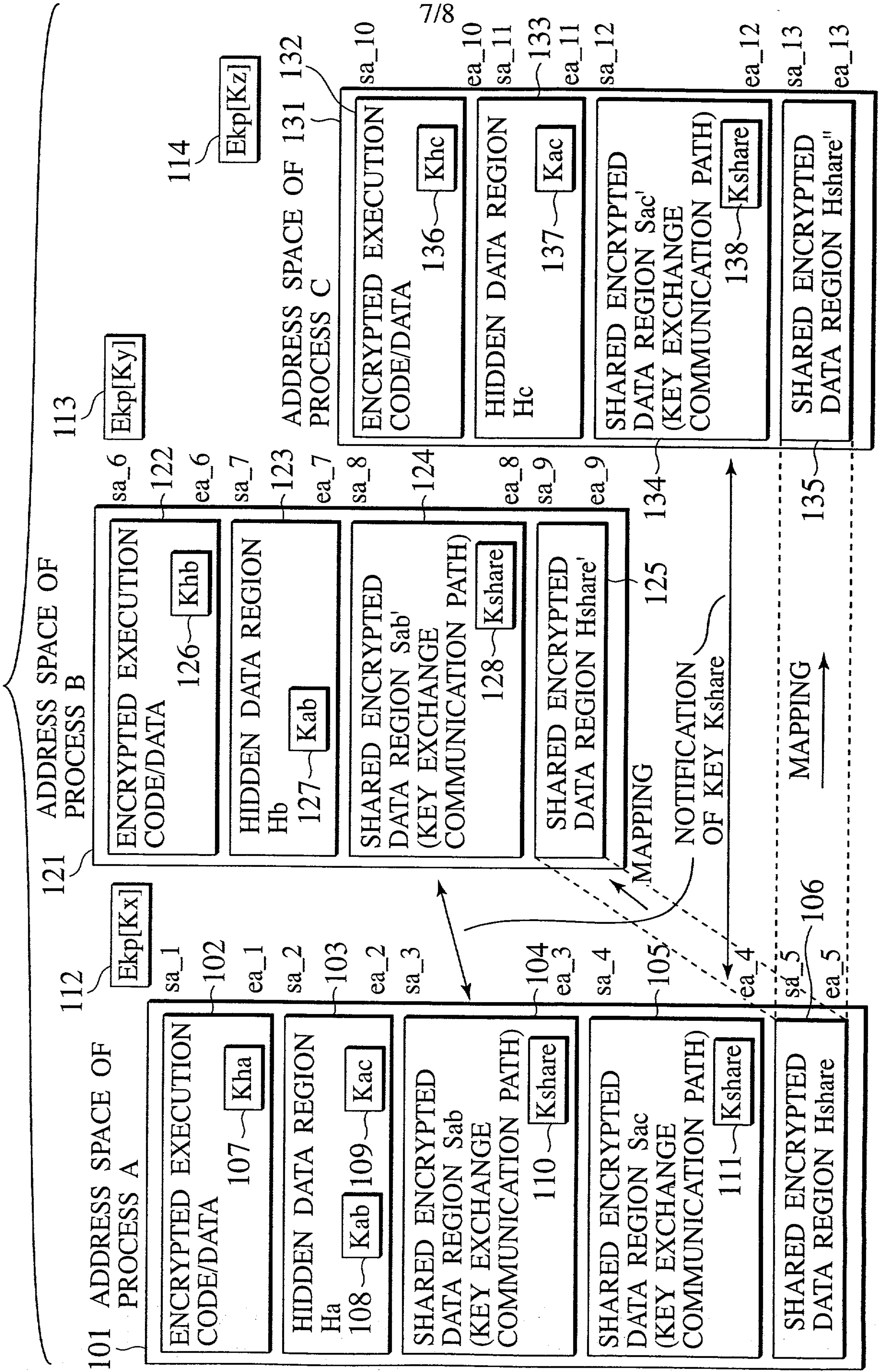
10028794.121801

FIG.6


PROCESS A
SENT BY USING METHOD PROVIDED BY OS
PROCESS B
SEND RANDOM NUMBER Bn & CERTIFICATE Bcert
VERIFY COMPLETENESS OF Bcert
SEND RANDOM NUMBER An & CERTIFICATE Acert
VERIFY COMPLETENESS OF Acert
CALCULATE KEY EXCHANGE 1ST PHASE Av
CALCULATE KEY EXCHANGE 1ST PHASE Bv
SEND Av BY ATTACHING SIGNATURE
VERIFY COMPLETENESS OF Av
SEND Bv BY ATTACHING SIGNATURE
VERIFY COMPLETENESS OF Bv
CALCULATE COMMON KEY Kab
CALCULATE COMMON KEY Kab

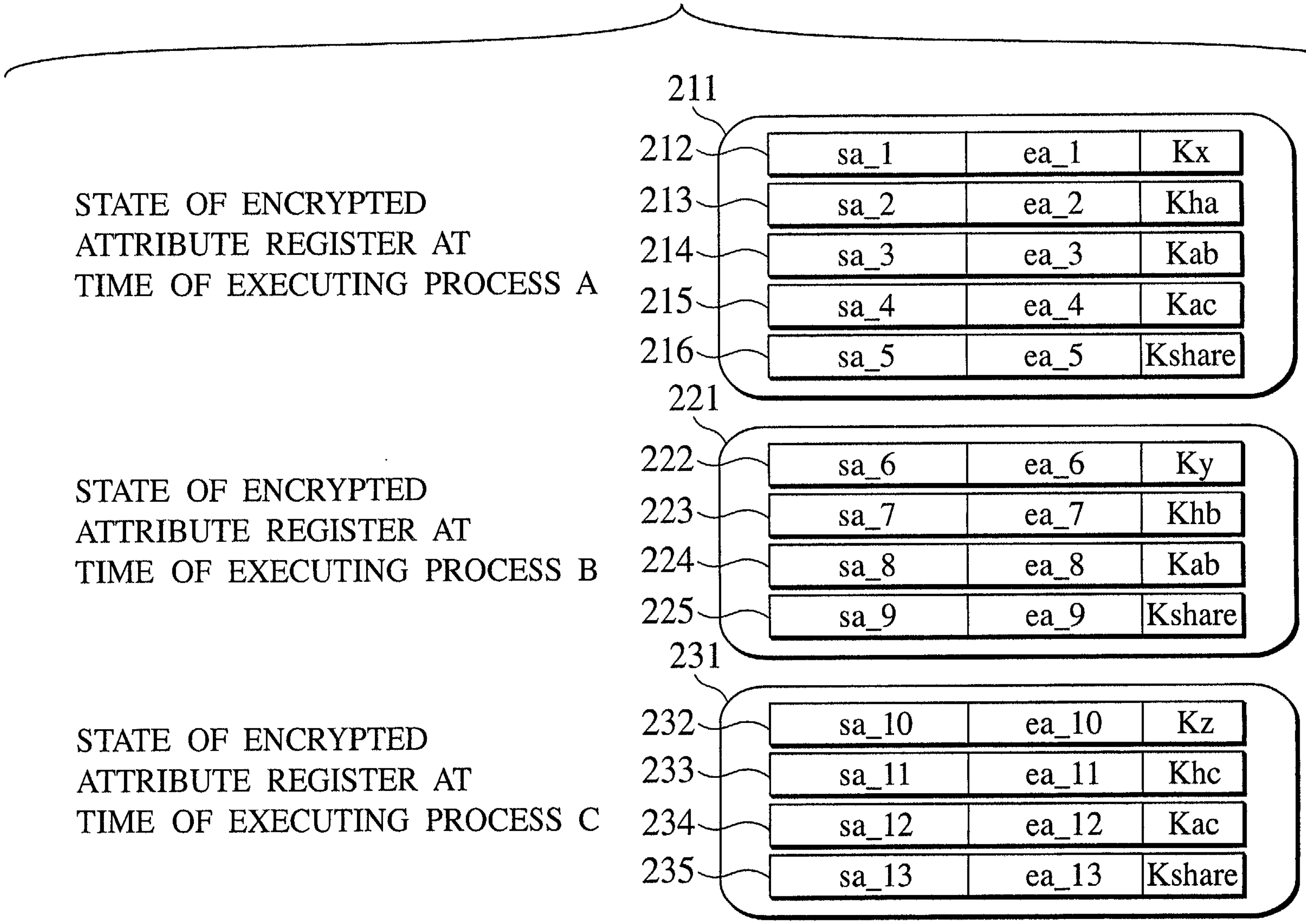
VERIFICATION, Av/Bv CALCULATION, SIGNATURE ATTACHING & COMMON KEY CALCULATION ALGORITHM EXECUTION ARE CARRIED OUT IN ENCRYPTED INSTRUCTION EXECUTION MODE, & TEMPORARY DATA ARE CREATED & STORED IN ENCRYPTED DATA REGION.

FIG.7


101
ADDRESS SPACE OF PROCESS A
112
Ekp[Kx]
sa_1
102
ea_1
ENCRYPTED EXECUTION CODE/DATA
107
Kha
sa_2
103
ea_2
HIDDEN DATA REGION Ha
108
Kab
109
Kac
sa_3
104
ea_3
SHARED ENCRYPTED DATA REGION Sab (KEY EXCHANGE COMMUNICATION PATH)
110
Kshare
sa_4
105
ea_4
SHARED ENCRYPTED DATA REGION Sac (KEY EXCHANGE COMMUNICATION PATH)
111
Kshare
sa_5
106
ea_5
SHARED ENCRYPTED DATA REGION Hshare
121
ADDRESS SPACE OF PROCESS B
113
Ekp[Ky]
sa_6
122
ea_6
ENCRYPTED EXECUTION CODE/DATA
126
Khb
sa_7
123
ea_7
HIDDEN DATA REGION Hb
127
Kab
sa_8
124
ea_8
SHARED ENCRYPTED DATA REGION Sab' (KEY EXCHANGE COMMUNICATION PATH)
128
Kshare
sa_9
ea_9
SHARED ENCRYPTED DATA REGION Hshare'
125
MAPPING
NOTIFICATION OF KEY Kshare
MAPPING
131
ADDRESS SPACE OF PROCESS C
114
Ekp[Kz]
132
sa_10
ea_10
ENCRYPTED EXECUTION CODE/DATA
136
Khc
sa_11
133
ea_11
HIDDEN DATA REGION Hc
137
Kac
sa_12
ea_12
SHARED ENCRYPTED DATA REGION Sac' (KEY EXCHANGE COMMUNICATION PATH)
138
Kshare
134
sa_13
ea_13
SHARED ENCRYPTED DATA REGION Hshare''
135

10082794.122801

FIG.8



STATE OF ENCRYPTED
ATTRIBUTE REGISTER AT
TIME OF EXECUTING PROCESS A

sa_1	ea_1	Kx
sa_2	ea_2	Kha
sa_3	ea_3	Kab
sa_4	ea_4	Kac
sa_5	ea_5	Kshare

STATE OF ENCRYPTED
ATTRIBUTE REGISTER AT
TIME OF EXECUTING PROCESS B

sa_6	ea_6	Ky
sa_7	ea_7	Khb
sa_8	ea_8	Kab
sa_9	ea_9	Kshare

STATE OF ENCRYPTED
ATTRIBUTE REGISTER AT
TIME OF EXECUTING PROCESS C

sa_10	ea_10	Kz
sa_11	ea_11	Khc
sa_12	ea_12	Kac
sa_13	ea_13	Kshare